DECISÃO COREN-SC N.º 046 DE 05 DE DEZEMBRO DE 2025

"Dispõe sobre o Plano de Gestão de Riscos à Integridade do Coren-SC".

A Presidente do Conselho Regional de Enfermagem de Santa Catarina (Coren-SC), em conjunto com a Primeira-Secretária da Autarquia, no uso de suas atribuições legais e regimentais conferidas pela Lei n.º 5.905 de 12 de julho de 1973, bem como pelo Regimento Interno da Autarquia, alterado pela Decisão Coren-SC n.º 050/2024, e homologado pela Decisão Cofen n.º 203/2024;

Considerando a Instrução Normativa (IN) Conjunta Ministério do Planejamento, Orçamento e Gestão (MPOG) e Controladoria-Geral da União (CGU) n.º 01/2016, que recomenda aos órgãos da administração pública a adoção de medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança;

Considerando o Decreto n.º 9.203/2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, e estabelece que os órgãos e as entidades da administração direta, autárquica e fundacional instituirão programa de integridade, com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção;

Considerando as recomendações do Tribunal de Contas da União (TCU) quanto à necessidade de adoção de mecanismos sistemáticos de identificação, avaliação, tratamento e monitoramento de riscos à integridade no âmbito da Administração Pública;

Considerando a Portaria CGU n.º 57, de 4 de março de 2019, que altera a Portaria CGU n.º 1.089/2018 e estabelece orientações para que os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional adotem procedimentos para a estruturação, execução e monitoramento de seus Programas de Integridade, dispondo, em seu art. 5º, inciso III, que o Plano de Integridade deve conter o levantamento dos principais riscos à integridade e as medidas para seu tratamento;

Considerando a Lei n.º 12.846, de 1º de agosto de 2013 (Lei Anticorrupção), que dispõe sobre a responsabilização objetiva administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública;

Considerando a importância da gestão de riscos à integridade como ferramenta de apoio à tomada de decisão, à prevenção de desvios éticos, à melhoria dos controles internos e ao fortalecimento da confiança da sociedade na atuação do Coren-SC;

Considerando a necessidade de institucionalizar práticas preventivas e integradas que fortaleçam o ambiente de controle, assegurem o cumprimento da missão institucional e minimizem a exposição a riscos que possam comprometer a integridade da Administração Pública;

Considerando a instituição do Escritório de Gestão da Integridade no âmbito do Coren-SC, conforme estrutura definida no Caderno de Atribuições do Regional, e;

Considerando a Política de Gestão de Riscos à Integridade do Coren-SC – Decisão Coren-SC n.º 045/2025;

Considerando por fim, a deliberação da Diretoria do Coren-SC em sua 47ª Reunião Ordinária;

Decidem:

Art. 1º Instituir o Plano de Gestão de Riscos à Integridade Coren-SC, na forma do Anexo a esta Decisão.

Art. 2º Esta Decisão entrará em vigor na data de sua assinatura.

Florianópolis, 05 de dezembro de 2025.

gov.br Documento assinado digitalmente
MARISTELA ASSUMPCAO DE AZEVEDO
Data: 09/12/2025 09:04:08-0300
Verifique em https://validar.iti.gov.br

Maristela Assumpção de Azevedo
Coren-SC n.º 033.234-ENF
Presidente

ICP Brasil Documento assinado digitalmente
SILVANA ALVES BENEDET OFUGI RODRIGUES
Data: 09/12/2025 09:49:51-0300
Verifique em https://validar.iti.gov.br

Silvana Alves Benedet Ofugi Rodrigues
Coren-SC n.º 60.207-ENF
Primeira-Secretária

PLANO DE GESTÃO DE RISCOS À INTEGRIDADE COREN-SC

Coren SC
Conselho Regional de Enfermagem de Santa Catarina

Plano de Gestão de Riscos à Integridade

Conselho Regional de Enfermagem de Santa Catarina – Coren-SC

Conteúdo

Gabriela Streck da Silva – Escritório de Gestão da Integridade – Coren-SC

Arte

Assessoria de Comunicação do Coren-SC

Florianópolis, setembro de 2025.

Gestão Enfermagem Valorizada e Participativa (2024-2026)

Diretoria
Presidente - Enfa. Maristela Assumpção de Azevedo
Vice-Presidente - Enfa. Sandra Regina da Costa
1ª Secretária – Enfa. Silvana Alves Benedet O. Rodrigues
2ª Secretária – Enfa. Ana Cristina Hoffmann
1ª Tesoureira – Téc. Enf. Fernanda Antunes Luz
Tesoureira - Téc. Enf. Henrique Manoel Alves

Conselheiros Efetivos
Enf. Everley Hobold
Enfa. Valdemira Santina Dagostin
Enfa. Poliana Weber Fontana
Enf. Tarcísio José da Silva
Téc. Enf. Ângelo Vidal Alves
Téc. Enf. Hanele Laske da Silva
Téc. Enf. Wallace Fernando Cordeiro

Conselheiros Suplentes
Enf. Dani Felipe Souza Pinto
Enfa. Denise Thum
Enf. Euclides da Cunha Correa
Enfa. Gabriele Carradore da Silva (licenciada)
Enfa. Maria Cristina Berta
Enfa. Tânia Silvana Schulz
Téc. Enf. Eliane Goulart Joaquim da Silva
Téc. Enf. Gleide Nara de Amorim
Téc. Enf. Junior da LuzWolff
Téc. Enf. Marilene Cagol Salles
Téc. Enf. Silvia Cristina Machado (licenciada)

SUMÁRIO

1.INTRODUÇÃO

Gestão de Riscos é um conjunto de atividades coordenadas que visa identificar, analisar, avaliar e tratar potenciais fragilidades que possam expor a organização a riscos, com o objetivo de fornecer segurança razoável quanto ao cumprimento de sua missão institucional e à realização de seus objetivos estratégicos.

Em conformidade com a Portaria CGU (Controladoria-Geral da União) n.º 57/2019 - altera a Portaria CGU n.º 1089/2018 - que estabelece orientações para que os órgãos e entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, execução e monitoramento de seus Programas de Integridade, e dispõe no seu art. 5º, III que o Plano de Integridade deve conter o levantamento dos principais riscos relacionados à integridade e estabeleça medidas para seu tratamento.

A elaboração do Plano de Integridade deve ser baseada na gestão dos riscos à integridade e na avaliação dos controles já existentes, com o objetivo de identificar vulnerabilidades no sistema de integridade da organização e propor ações eficazes para mitigar esses riscos.

O Escritório de Gestão da Integridade (EGI) será responsável pela coordenação do processo de gestão de riscos à integridade no Coren-SC, com o intuito de identificar, junto às Unidades Funcionais do Conselho, possíveis fragilidades que possam facilitar a ocorrência de fraude, corrupção ou desvios éticos e de conduta. A partir dessa identificação, serão estabelecidas ações preventivas e de contingência voltadas ao fortalecimento da cultura de integridade, à garantia da conformidade institucional, à promoção da transparência e à observância dos princípios éticos e legais em todas as atividades e processos organizacionais.

A Controladoria Geral da União (CGU), em seu Guia Prático para a Gestão de Riscos para a Integridade, aponta algumas áreas e grupos suscetíveis a riscos à integridade, incluindo: compras públicas, acordos e convênios, gestão patrimonial, gestão de pessoas, ouvidoria, diárias e passagens, alta direção, concessão de créditos, fiscalização, colegiados e atendimento ao público.

Como pode ser observado, essas áreas são comuns à maioria dos órgãos públicos e estão relacionadas aos segmentos administrativos. Portanto, devem ser consideradas com atenção no processo de riscos à integridade. No entanto, além desses exemplos muito comuns, cada

organização tem processos específicos relacionados às suas competências e atividades. Esses processos também precisam ser analisados sob a perspectiva de riscos à integridade, especialmente porque em sua maioria, estão associados às áreas finalísticas das organizações, ou seja, àqueles segmentos cujos produtos e resultados representam entregas à sociedade ou ao seu público-alvo, de forma direta ou indireta.

No contexto da gestão de riscos à integridade, a facilitação de fraudes e atos de corrupção não se restringe ao descumprimento de leis e normas, abrangendo também outras situações que comprometem a integridade, como a falta de transparência, a omissão de informações relevantes, a manipulação de processos decisórios, o abuso de poder ou a permissividade diante de comportamentos antiéticos.

De um modo geral, atos relacionados a quebras de integridade compartilham das seguintes características:

- É um ato quase sempre doloso, à exceção de certas situações envolvendo conflito de interesses, nepotismo, etc;
- É um ato humano, praticado por uma pessoa ou um grupo de pessoas;
- Envolve uma afronta aos princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência, mas se destaca mais fortemente como uma quebra à impessoalidade e/ou moralidade;
- Envolve alguma forma de deturpação, desvio ou negação da finalidade pública ou serviço público a ser entregue ao cidadão.

A partir dessas características, em uma listagem não exaustiva, a CGU aponta alguns **riscos à integridade mais relevantes nas organizações públicas**:

- **Abuso de posição ou poder em favor de interesses privados**: adoção de conduta incompatível com o interesse público, utilizando-se da posição ocupada para favorecer interesses privados, em benefício próprio ou de terceiros.

- **Comportar-se de forma incompatível com a função pública**: adoção de condutas, dentro ou fora do ambiente de trabalho, que violam princípios éticos e legais, comprometendo a confiança, a imparcialidade e a imagem da administração pública;

- **Conflito de interesses**: situação gerada pelo confronto de interesses públicos e privados,

que possa comprometer o interesse coletivo e influenciar, de maneira imprópria, o desempenho da função pública. Ex.: divulgar ou fazer uso de informações privilegiadas em proveito próprio ou de terceiros, obtida em razão das atividades exercidas;

- **Exercer pressão interna ou externa ilegal ou antiética para influenciar agente público/privado**: pressionar agente público a agir de maneira parcial, antiética ou ilegal. Essa pressão pode ser implícita ou explícita, interna ou externa à organização;

- **Nepotismo:** ocorre quando um agente público usa de sua posição ou poder para nomear, contratar ou favorecer parentes em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

- **Solicitação ou recebimento de vantagem indevida:** obtenção indevida de dinheiro ou qualquer outra vantagem, direta ou indireta, em razão do cargo ou função exercida, configurando enriquecimento ilícito, vedado ao agente público no desempenho de suas atribuições;

- **Utilização de verbas e fundos públicos em favor de interesses privados:** trata-se do uso indevido de recursos públicos para beneficiar pessoas, empresas ou grupos específicos, em vez de atender ao interesse coletivo, o que configura desvio de finalidade e afronta aos princípios da administração pública;

- **Utilização/vazamento de informação privilegiada/restrita:** consiste no uso ou divulgação indevida de informações sigilosas obtidas em razão do cargo ou função, com o objetivo de beneficiar a si próprio ou a terceiros, em prejuízo da equidade, da ética e do interesse público.

A identificação e o tratamento de riscos à integridade não devem ser vistos apenas sob a ótica punitiva ou reativa. Em um modelo de governança pública orientado por boas práticas, os riscos representam também oportunidades estratégicas de melhoria, inovação e fortalecimento institucional.

Situações que colocam em risco a integridade — como fragilidades em controles internos, lacunas normativas, falhas em processos ou comportamentos antiéticos — funcionam como alertas para a necessidade de aprimoramento contínuo da gestão pública. Quando bem identificados e tratados, esses riscos possibilitam a revisão de práticas, a modernização de

sistemas, o reforço da cultura ética e o aumento da transparência e da confiança social.

Além disso, a abordagem preventiva adotada pela gestão de riscos contribui para a criação de ambientes mais seguros, íntegros e resilientes, nos quais a administração pública se antecipa aos problemas e atua de forma proativa. Assim, o tratamento de riscos à integridade torna-se também uma oportunidade para inovar, otimizar recursos, elevar padrões de governança e garantir a entrega de serviços públicos com maior qualidade e legitimidade.

Uma vez concretizados, os riscos à integridade podem prejudicar significativamente a organização, dificultando a consecução de seus objetivos, enfraquecendo a confiança pública e institucional, e comprometendo sua reputação e eficácia. Além disso, esses riscos afetam diretamente a credibilidade dos agentes públicos envolvidos, podendo acarretar responsabilidades em diversas esferas.

Portanto, promover a integridade na administração pública requer uma gestão de riscos eficaz, capaz de identificar, avaliar e mitigar vulnerabilidades que possam comprometer a legalidade, a moralidade e a eficiência na gestão dos recursos públicos, contribuindo para a prevenção de irregularidades, a salvaguarda do interesse coletivo e o fortalecimento da confiança da sociedade nas organizações.

2. OBJETIVO

Este Plano tem por objetivo apresentar a metodologia a ser aplicada no Processo de Gestão de Riscos à Integridade no Coren-SC, promovendo sua aplicação conforme as diretrizes estabelecidas na Política de Gestão de Riscos à Integridade.

A gestão de riscos à integridade tem como objetivo assegurar que as práticas administrativas e operacionais dos agentes públicos sejam conduzidas com ética, transparência e responsabilidade. Essa abordagem busca minimizar riscos associados a práticas inadequadas, como corrupção, favorecimento, conflitos de interesse, abuso de poder ou falhas na gestão pública, garantindo a boa execução dos processos e a confiança da sociedade nas ações do Conselho.

Para atingir esse abjetivo, é fundamental criar um ambiente de trabalho em conformidade com a legislação vigente, as normas éticas da administração pública e as diretrizes internas do Conselho, garantindo que os agentes públicos atuem com integridade e de acordo com os

princípios constitucionais da moralidade, impessoalidade, publicidade e eficiência.

Adotar uma abordagem preventiva e proativa não apenas protege a reputação do Conselho, mas também preserva a integridade dos agentes públicos, assegurando que suas funções sejam desempenhadas de forma eficiente, transparente e em conformidade com as normas legais. Esse compromisso com a integridade contribui para consolidar a credibilidade do Coren-SC perante a sociedade.

3. APLICABILIDADE

A aplicação do Plano de Gestão de Riscos à Integridade ocorrerá de forma gradual em todas as Unidades Funcionais do Coren-SC, respeitando-se, em paralelo, a aplicação de normativos complementares específicos que regulamentam os processos de trabalho, projetos e ações de cada Unidade.

4. TERMOS E DEFINIÇÕES

Conforme disposto no art. 4º da Política de Gestão de Riscos à Integridade, aprovada pela Decisão Coren-SC n.º 45/2025.

5. COMPETÊNCIAS E RESPONSABILIDADES

Conforme disposto nos arts. 8º a 14 da Política de Gestão de Riscos à Integridade, aprovada pela Decisão Coren-SC n.º 45/2025.

6. DEFINIÇÃO DO APETITE A RISCOS

Antes de iniciar o Processo de Gestão de Riscos à Integridade, é fundamental definir, junto à Diretoria do Coren-SC, com aprovação do Plenário (Alta Administração), o apetite ao risco — ou seja, o nível de risco que a organização está disposta a aceitar no exercício de suas atividades, considerando seus objetivos estratégicos, sem a necessidade de medidas adicionais de mitigação. Estabelecer esses limites é crucial paraprevent a avaliação eficaz dos riscos e para a definição de ações de tratamento apropriadas. Essa definição orienta a priorização dos riscos que exigem atenção imediata, de forma a equilibrar oportunidades e ameaças no alcance dos resultados institucionais Importante ressaltar que o apetite a risco é dinâmico, podendo ser modificado de acordo com o contexto e situação percebida em um dado momento.

7. PROCESSO DE GESTÃO DE RISCOS À INTEGRIDADE

O Processo de Gestão de Riscos à Integridade abrange as seguintes etapas:

- Estabelecimento do contexto;
- Identificação dos riscos;
- Análise dos riscos;
- Avaliação dos riscos;
- Tratamento dos riscos;
- Monitoramento;
- Análise crítica e melhoria contínua;
- Comunicação e consulta;
- Registro e relato.

Essas etapas estão ilustradas a seguir:

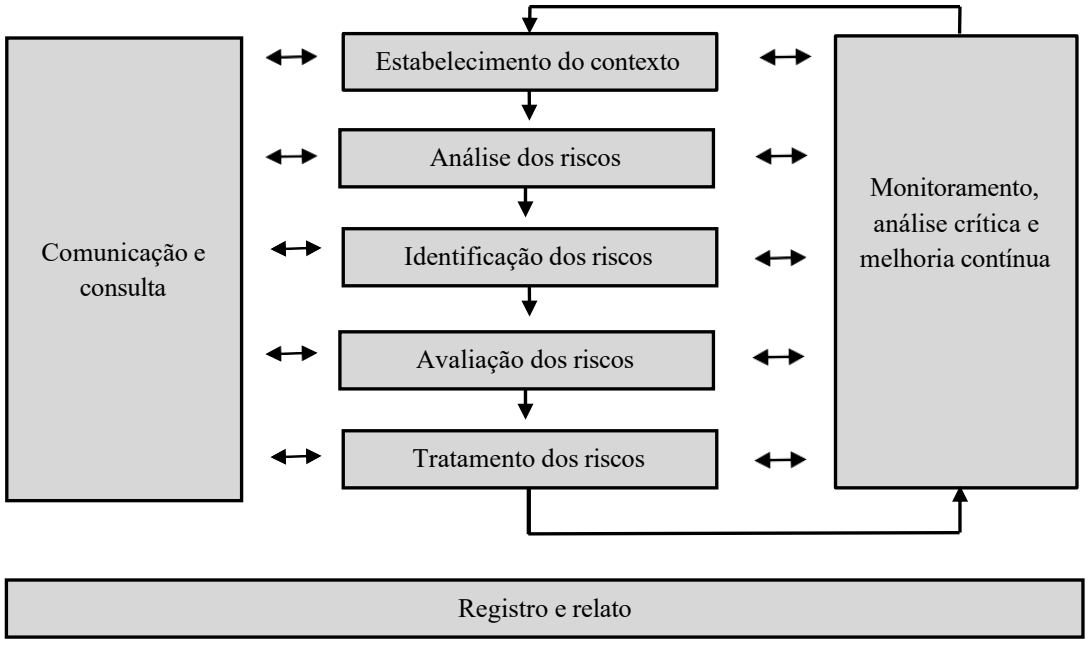

Figura 1: Processo de Gestão de Riscos da ISO 31000, adaptado

Para que o processo seja implementado de forma eficaz, é essencial a participação ativa das Unidades Funcionais do Coren-SC, envolvendo a colaboração de pessoas de todos os níveis de execução das atividades, que possuam um bom conhecimento sobre o objeto da gestão de riscos à integridade, ou seja, os processos de trabalho, as atividades, os projetos, as iniciativas, as ações do plano institucional e os recursos que sustentam a realização dos objetivos da organização. A diversidade de especialidades e níveis hierárquicos garante que diferentes

perspectivas sejam consideradas, enriquecendo a análise dos riscos. Além disso, essa diversidade é fundamental para assegurar a transparência e a inclusão em todo o processo. Outro fator crucial para o sucesso da implementação é o apoio irrestrito da Alta Administração.

Para identificar, analisar e avaliar os riscos à integridade, bem como definir as medidas de tratamento adequadas para os riscos levantados, serão realizadas reuniões com as equipes das Unidades Funcionais do Coren-SC, utilizando a técnica de brainstorming (tempestade de ideias). Essa técnica tem como objetivo explorar o potencial criativo dos participantes, permitindo que todos contribuam com ideias acerca de um determinado tema sem sofrer nenhum tipo de crítica.

Durante as reuniões é importante incentivar e proporcionar espaço para que divergências de interpretação e opinião sejam expressas, assim como para lidar com incertezas e limitações de informações sobre o processo. O objetivo é garantir que a equipe de cada Unidade Funcional trabalhe para esclarecer dúvidas e construir um entendimento comum.

As informações coletadas serão registradas no módulo de Gestão de Riscos da Plataforma Tecnológica de Compliance, garantindo a padronização e a segurança dos dados.

A Encarregada da Gestão da Integridade será responsável por coordenar o processo de gestão de riscos à integridade, desempenhando uma função preponderantemente de assessoramento e acompanhamento/supervisão nas diversas etapas desse processo. De acordo com a CGU, a Unidade de Gestão da Integridade atua principalmente como órgão de apoio, oferecendo suporte à alta administração e às demais áreas, além de exercer um papel facilitador na divulgação de práticas e processos que contribuam para a incorporação do sistema de gestão de riscos na organização.

7.1 ESTABELECIMENTO DO CONTEXTO

O propósito do estabelecimento do contexto é compreender o ambiente interno e externo onde os riscos à integridade podem surgir. Isso permite uma visão ampla da organização, suas metas e vulnerabilidades, servindo de base para identificar e priorizar os riscos à integridade com mais precisão, orientando, assim, a implementação de medidas de mitigação eficazes. Nessa etapa, são utilizadas técnicas específicas que servirão de base para as próximas etapas do processo de gestão de riscos à integridade.

Uma das técnicas adotadas será o levantamento dos processos de trabalho existentes, a ser realizado por meio de um formulário gerado na Plataforma Tecnológica de Compliance. Esse formulário, acessado por meio de um link da Plataforma Tecnológica de Compliance (Anexo III), será enviado aos Coordenadores das Unidades Funcionais do Coren-SC, com prazo previamente estabelecido para o envio das respostas. As Unidades deverão preencher as informações solicitadas e anexar uma planilha em Excel com os dados do levantamento, conforme o modelo do Anexo III. Essa planilha será encaminhada separadamente por e-mail aos Coordenadores. As respostas inseridas no formulário serão automaticamente registradas na Plataforma, assegurando o armazenamento e a organização das informações de maneira eficiente e precisa.

Além do levantamento dos processos de trabalho existentes, outra técnica que será empregada é a matriz *SWOT (Strenghts, Weaknesses, Opportunitiesand Threats)* ou FOFA (Forças, Oportunidades, Fraquezas e Ameaças), uma ferramenta estratégica que permite avaliar fatores internos e externos que podem impactar o desempenho de uma organização.

Essa abordagem foi aplicada às Unidades Funcionais em junho de 2024, com o objetivo de elaborar o Plano Plurianual – Gestão 2024-2026, e os resultados obtidos serão utilizados no estabelecimento do contexto para o processo de gestão de riscos à integridade. Como essa análise foi realizada há quase um ano, o cenário descrito pelas Unidades na matriz FOFA pode ter sofrido alterações, tanto positivas quanto negativas. Por isso, no formulário que será enviado às Unidades Funcionais, será questionado se houve alguma modificação no cenário apresentado na matriz FOFA de 2024. Caso haja uma resposta afirmativa, as alterações deverão ser descritas.

Além das técnicas mencionadas, para o estabelecimento do contexto, podem ser averiguados casos pretéritos de quebra de integridade, bem como consultas a documentos como o planejamento estratégico, relatórios de gestão, prestação de constas, relatórios de auditorias internas e externas e qualquer outra documentação pertinente à organização e suas finalidades.

Estabelecido o contexto, o processo de identificação dos principais riscos à integridade torna-se mais claro e direcionado, facilitando a avaliação dos aspectos mais relevantes e críticos para a Unidade Funcional, além de permitir a priorização adequada das ações de mitigação e tratamento.

7.2 IDENTIFICAÇÃO DOS RISCOS

Identificação de riscos é um processo que visa reconhecer e descrever os eventos que envolvem possíveis riscos à integridade aos quais a organização está exposta, identificando suas fontes, causas e possíveis consequências.

Nesta etapa, o objetivo é identificar os eventos de riscos à integridade que possam impactar os processos de trabalho, as atividades, os projetos, as iniciativas, as ações do plano institucional e os recursos que sustentam a realização dos objetivos da organização, os quais são o foco da gestão de riscos.

As ferramentas para a identificação de riscos à integridade devem considerar, por um lado, os princípios fundamentais que regem a Administração Pública, bem como os normativos sobre deveres, proibições, valores éticos e morais, englobando todo o conjunto normativo que orienta a gestão pública e as condutas de seus agentes. Por outro lado, devem levar em conta as características inerentes às atividades organizacionais, processos de trabalho, bases e sistemas de informações, interações com partes interessadas e tecnologias utilizadas. Os elementos-chave para identificação dos riscos à integridade são aqueles levantados na etapa anterior, ou seja, no estabelecimento do contexto.

Com base no levantamento dos processos de trabalho enviado pelas Unidades Funcionais e nos resultados da matriz FOFA das Unidades, a Encarregada da Gestão da Integridade - responsável pela coordenação do processo de gestão de riscos à integridade - realizará a identificação preliminar dos riscos associados a cada Unidade. Esses riscos serão encaminhados previamente, por e-mail, aos coordenadores das respectivas Unidades, para conhecimento e análise prévia. Em seguida, serão discutidos nas reuniões com as equipes das Unidades, com o objetivo de validar os riscos identificados e permitir a inclusão de outros que sejam considerados relevantes.

Após o reconhecimento e a descrição dos riscos à integridade, é necessário apontar suas causas e possíveis consequências. Causa refere-se a qualquer fator, ação ou omissão que contribua para a ocorrência de um evento de risco, seja por provocar diretamente sua materialização ou por criar condições favoráveis para que ele aconteça. Consequência é o impacto negativo gerado pela materialização de um evento de risco, que pode comprometer os objetivos da organização, afetando sua integridade institucional, reputação, recursos, processos ou sua capacidade de cumprir sua missão. Vale destacar que um risco pode ter

múltiplas causas e/ou consequências, e que uma mesma causa ou consequência pode estar relacionada a diferentes riscos. Ademais, os riscos à integridade podem ser causa ou consequência de outras categorias de riscos, como operacionais, financeiros ou de imagem.

Existem alguns fatores de risco à integridade que podem dar causa à manifestação de um risco à integridade:

- **Fatores de risco externos:** fatores que se encontram fora do controle da organização e aos quais ela deve estar atenta. Exemplos: alterações de legislação, a invasão de sistemas digitais do Conselho por hackers ou a falha de sistemas de gestão de dados pode comprometer o acesso a informações importantes sobre o cadastro de profissionais, seus registros e infrações cometidas, prejudicando a transparência e a eficácia na fiscalização, entre outros;

- **Fatores de risco organizacionais:** fatores sob controle da organização, como resultado de suas ações ou inações. Exemplos: o não cumprimento ou a falha em atualizar normas e regulamentos; o mau gerenciamento dos recursos financeiros; falta de transparência nas decisões ou procedimentos; entre outros;

- **Fatores de risco individuais:** fatores que surgem das motivações individuais dos agentes públicos para o cometimento de atos que afrontem as regras de integridade. Exemplos: um agente público do Conselho que também exerça atividades profissionais na área que regula ser influenciado por seus interesses pessoais ao tomar decisões que favoreçam instituições, sua própria carreira ou a de colegas próximos; falta de capacitação dos agentes públicos; manipulação de registros de profissionais ou alteração informações nos processos de fiscalização ou licitatórios para beneficiar determinados indivíduos ou empresas; divulgação de informações sigilosas/reservadas para terceiros; entre outros.

A CGU apresenta um rol exemplificativo dos fatores dos riscos mais comuns:

- Legislação e normas internas imprecisas ou omissas;
- Não observância de legislação/normas internas;
- Pressões organizacionais verticais (hierárquicas) e horizontais (colegas de trabalho);
- Ausência/deficiência de sistemas informatizados;
- Ausência/deficiência de controles hierárquicos;
- Ausência/deficiência de mecanismos de controle interno;

- Ausência/deficiência de planejamento estratégico e operacional;
- Ausência/deficiência de segregação de funções sensíveis;
- Ausência/deficiência de recursos humanos/orçamentários;
- Desconhecimento de normas/procedimentos pelos agentes públicos;
- Desconhecimento de normas/procedimentos pela população atendida;
- Ausência/deficiência de políticas de transparência e controle social;
- Fragilidades em estimativas de valores/quantitativos de bens/serviços;
- Impunidade ou sentimento de impunidade entre os agentes públicos;
- Ingerências externas nas atividades da organização;
- Gestão incorreta de documentos/processos.

Exemplo hipotético de risco à integridade, bem como suas causas e consequências:

IDENTIFICAÇÃO DOS RISCOS À INTEGRIDADE			
Risco	**Descrição do Risco**	**Causas**	**Consequências**
Solicitação ou recebimento de vantagens indevidas	Solicitação de vantagem para favorecer determinada empresa em uma contratação	1) Desconhecimento do Código de Conduta Ética da organização;	1) Prejuízo à qualidade e eficiências dos serviços, ao favorecer uma empresa sem qualificação ou capacidade;
		2) Falta de ações preventivas;	2) Prejuízo ao erário ao favorecer uma empresa com preço superior ao de outras empresas;
		3) Falhas no controle interno;	3) Desgaste da imagem e perda da credibilidade institucional;
		4) Conflito de interesses;	4) Consequências legais e administrativas;
		5) Cultura organizacional deficiente.	5) Dano à imparcialidade do processo.

Tabela 1: Exemplo hipotético risco à integridade, suas causas e consequências

Uma vez identificados os riscos à integridade, avançaremos para a próxima etapa, que consiste na análise dos riscos.

7.3 ANÁLISE DOS RISCOS

A etapa de análise dos riscos visa compreender a natureza dos riscos à integridade, levando em consideração as causas e consequências identificadas na etapa anterior, e determinar o nível de risco. Nesta etapa, os níveis dos riscos serão estimados e mensurados em duas etapas:

1. Definição do Nível de Risco Inerente (NRI), e

2. Definição do Nível de Risco Residual (NRR).

A análise de riscos servirá como base para a avaliação e o tratamento dos riscos à integridade levantados.

7.3.1 Definição do Nível de Risco Inerente (NRI)

A primeira etapa da análise de riscos consiste na definição do Nível de Risco Inerente (NRI), ou seja, o nível de riscos sem considerar quaisquer ações de controles destinados ao enfrentamento dos riscos levantados.

Para cada risco à integridade identificado, será necessário mensurar a Probabilidade (P) de sua ocorrência e o Impacto (I) que esse risco terá nos objetivos da organização, caso venha a se materializar. Essas mensurações deverão seguir os critérios estabelecidos nas Tabelas 2 e 3 abaixo:

a) Análise e mensuração da Probabilidade (P)

Para a análise da Probabilidade, será utilizada uma escala de níveis de 1 a 5, com critérios definidos para cada nível, conforme a tabela abaixo:

ESCALA DE PROBABILIDADE		
Probabilidade	**Descrição**	**Nível**
Muito Baixa	**Rara:** em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	**Improvável:** de forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	**Possível:** de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3
Alta	**Provável:** de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito Alta	**Praticamente certa:** de forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	5

Tabela 2: Escala de Probabilidade.

b) Análise e mensuração do Impacto (I)

Para a análise do Impacto, será utilizada uma escala de níveis de 1 a 5, com critérios definidos para cada nível, conforme a tabela abaixo:

ESCALA DE IMPACTO		
Impacto	**Descrição**	**Nível**
Muito Baixo	**Impacto insignificante** nos objetivos.	1
Baixo	**Impacto mínimo** nos objetivos.	2
Médio	**Moderado impacto** nos objetivos, porém recuperável.	3
Alto	**Significativo impacto** nos objetivos, de difícil recuperação.	4
Muito Alto	**Catastrófico impacto** nos objetivos, sem possibilidade de recuperação.	5

Tabela 3: Escala de Impacto.

c) Cálculo do Nível de Risco Inerente (NRI):

Após a mensuração dos níveis de Probabilidade (P) e Impacto (I), o Nível de Risco Inerente (NRI) pode ser calculado por meio do produto aritmético entre essas duas variáveis, conforme a fórmula a seguir:

NRI = P x I

Esse cálculo permitirá classificar o risco à integridade de acordo com seu nível de gravidade.

d) Classificação do Nível de Risco Inerente (NRI):

Para a classificação do Nível de Risco Inerente (NRI), será utilizada a Matriz de Riscos (Figura 2), com a escala de Probabilidade (P) x Impacto (I) no formato 5x5 (cinco por cinco). Essa matriz delimitará quatro classificações de níveis de risco, a partir da combinação entre os níveis de probabilidade e impacto: baixo, médio, alto e extremo. Os critérios específicos para cada nível de risco estão detalhados na Escala de Níveis de Risco Inerente, conforme apresentado na Tabela 4.

		IMPACTO (I)				
		Muito baixo (1)	**Baixo (2)**	**Médio (3)**	**Alto (4)**	**Muito alto (5)**
PROBABILIDADE (P)	**Muito alto (5)**	Risco médio **5**	Risco médio **10**	Risco alto **15**	Risco extremo **20**	Risco extremo **25**
	Alto (4)	Risco baixo **4**	Risco médio **8**	Risco alto **12**	Risco alto **16**	Risco extremo **20**
	Médio (3)	Risco baixo **3**	Risco médio **6**	Risco médio **9**	Risco alto **12**	Risco alto **15**
	Baixo (2)	Risco baixo **2**	Risco baixo **4**	Risco médio **6**	Risco médio **8**	Risco médio **10**
	Muito baixo (1)	Risco baixo **1**	Risco baixo **2**	Risco baixo **3**	Risco baixo **4**	Risco médio **5**

Figura 2: Matriz de riscos

O produto aritmético entre as duas medidas (P x I) gera um valor numérico para cada célula da matriz, variando de 1 a 25, que representa o Nível de Risco Inerente (NRI). A matriz organiza os possíveis níveis de risco, refletindo sua criticidade ou magnitude, desde o nível mais baixo (1), que corresponde a um evento muito raro e de impacto muito baixo, até o nível mais elevado (25), que representa um evento praticamente certo e de impacto muito alto.

Quanto maior a probabilidade e o impacto, maior será o nível de risco inerente. Com o resultado obtido na matriz, será possível classificar o risco de acordo com a faixa em que ele se enquadre, conforme Escala de Níveis de Risco Inerente abaixo:

Escala de Níveis de Risco Inerente (P x I)	
Classificação	**Faixa**
Risco baixo	1 a 4
Risco médio	5 a 10
Risco alto	12 a 16
Risco extremo	20 a 25

Tabela 4: Escala de Níveis de Risco Inerente

Exemplo:

Risco	P	I	NRI (P x I)	Classificação NRI
X	3	4	12	Risco alto

Tabela 5: Exemplo Nível de Risco Inerente (NRI).

7.3.2 Definição do Nível do Risco Residual (NRR)

Após a definição do Nível de Risco Inerente (NRI), a segunda etapa da análise dos riscos consiste na definição do Nível do Risco Residual (NRR), ou seja, o nível de risco remanescente, considerando os controles já implementados para o enfrentamento dos riscos à integridade levantados.

a) Identificação da existência de controles

Para a definição do Nível de Risco Residual (NRR), é necessário, primeiramente, identificar a existência de controles internos no Coren-SC voltados para o enfrentamento dos riscos à integridade levantados.

Os controles internos consistem em um conjunto de regras, diretrizes, normativos internos, políticas, manuais, rotinas de sistemas informatizados, conferências, trâmites de documentos informações, entre outros. Estes controles são implementados de forma integrada pelos agentes públicos da organização, com o objetivo de mitigar os riscos à integridade e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam atingidos de maneira eficaz, eficiente, efetiva e econômica.

Quando as atividades de controle são estabelecidas de maneira tempestiva e adequada, elas possuem o potencial de prevenir ou gerenciar os riscos inerentes à organização. Esses controles não são exclusivos de uma área específica, mas devem ser executados em todos os níveis da estrutura organizacional.

São exemplos de tipologias de atividades de controle: atribuição de autoridade e limites de alçada; revisão de superiores; normatização interna; autorizações e aprovações; controles físicos; segregação de funções; capacitação e treinamento; verificações; checklist; conciliações; indicadores de desempenho; restrições de sistemas.

b) Análise e mensuração da eficácia dos controles internos existentes

Após a identificação dos controles internos existentes, é fundamental classificá-los em termos de sua eficácia, ou seja, avaliar se têm contribuído adequadamente para o tratamento dos riscos à integridade identificados. Essa avaliação será quantificada por meio do Fator de Avaliação dos Controles (FAC), com base em uma tabela que classifica o desempenho de cada controle:

Eficácia dos Controles	Identificação dos controles existentes	Fator de Avaliação dos Controles (FAC)
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1,0
Fraco	Controles têm abordagem *ad hoc*, tendem a ser aplicados caso a caso; a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a melhor prática, mitigando todos os aspectos relevantes ao risco.	0,2

Tabela 6: Definição da eficácia dos controles.

c) Cálculo do Nível de Risco Residual (NRR):

Após a análise e mensuração da eficácia dos controles internos existentes, será possível calcular o **Nível de Risco Residual (NRR)**. Para isso, deve-se multiplicar o Nível de Risco Inerente (NRI), obtido na primeira etapa, pelo Fator de Avaliação dos Controles (FAC), conforme a fórmula a seguir:

NRR = NRI x FAC

d) Classificação do Nível de Risco Residual (NRR):

Com o resultado do cálculo do Nível de Risco Residual (NRR), será possível classificar o seu nível, utilizando como base a **Escala de Níveis de Risco Residual** apresentada abaixo:

Escala de Níveis de Risco Residual (NRR = NRI x FAC)	
Classificação	**Faixa**
Risco baixo	1 a 4,9
Risco médio	5 a 11,9
Risco alto	12 a 19,9
Risco extremo	20 a 25

Tabela 7: Escala de Níveis de Risco Residual.

Exemplo:

Risco	P	I	NRI (P x I)	Classificação NRI	FAC	NRR (NRI x FAC)	Classificação NRR
X	3	3	9	Risco médio	0,4	3,6	Risco baixo

Tabela 8: Exemplo Nível de Risco Residual (NRR).

O valor do risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente daquela definida para o risco inerente. No exemplo em questão, observa-se que o risco foi reduzido de nível médio para nível baixo após a aplicação dos controles internos.

A partir da análise dos riscos, é possível obter uma visão geral dos níveis de risco associados a cada ameaça à integridade identificada, permitindo, assim, estabelecer a prioridade para o tratamento na próxima etapa.

7.4. AVALIAÇÃO DOS RISCOS

Após a análise dos riscos à integridade, essa etapa tem como foco definir quais riscos serão priorizados para tratamento e qual tipo de resposta é mais apropriada para cada situação. Com base nos níveis de riscos residuais calculados, serão avaliadas decisões como:

- Determinar se um risco específico necessita de tratamento e com qual prioridade;
- Definir se uma atividade associada ao risco será mantida, ajustada ou encerrada;
- Avaliar se os controles atuais são suficientes ou se precisam ser aprimorados.

A priorização dos riscos seguirá o apetite ao risco definido pela Alta Administração:

- **Riscos acima do limite aceitável** devem ser tratados e monitorados com maior atenção, sendo necessária uma justificativa para a ausência de ações de tratamento;

- **Riscos dentro do limite aceitável** podem continuar sendo gerenciados com os controles existentes — mas, se forem priorizados para tratamento, a decisão deve ser justificada.

7.5 TRATAMENTO DOS RISCOS

O objetivo desta etapa é definir as medidas de resposta para o tratamento dos riscos à integridade classificados como prioritários, com foco na redução de seu nível a patamares aceitáveis.

Na definição das medidas de resposta, é essencial realizar uma análise detalhada de custo-benefício, levando em consideração não apenas a aplicabilidade e a eficácia das medidas/controles propostos, mas também os benefícios tangíveis e intangíveis que serão agregados ao processo. Além disso, deve-se avaliar a viabilidade de implementação, o tempo necessário para a adoção das medidas e os recursos disponíveis, assegurando que as soluções escolhidas sejam sustentáveis a longo prazo e proporcionem a melhor relação entre o custo de implementação e os benefícios alcançados.

A definição das medidas de tratamento envolve os seguintes procedimentos:

- **Selecionar as medidas de resposta** a serem adotadas para cada risco à integridade identificado, analisado e avaliado, com o objetivo de reduzir o nível do risco;
- **Estabelecer ações preventivas e de contingência**, quando necessário, para evitar, mitigar ou transferir os riscos de forma eficaz;
- **Indicar os responsáveis** por cada ação de tratamento;
- **Definir prazos** para a implementação das ações estabelecidas, garantindo que o tratamento seja realizado de forma tempestiva e eficiente.

As medidas de resposta para o tratamento dos riscos são:

- **Aceitar**: quando a organização decide assumir o risco, sem adoção de ações adicionais, por considerá-lo dentro dos limites aceitáveis definidos. Sua probabilidade e impacto são tão baixos que não justificam a implementação de novos controles. Em vez disso, pode optar por manter os controles existentes, que já são suficientes para minimizar as consequências do risco.

- **Transferir**: quando a probabilidade e o impacto do risco são elevados e a organização não pode suportá-los, ela opta por transferir o risco para outra parte. Isso pode ser feito por

meio de contratos, acordos ou seguros, transferindo a responsabilidade ou as consequências financeiras do risco. Ex.: a contratação de uma empresa de consultoria para realizar auditoria interna para maior imparcialidade, independência.

- **Mitigar**: quando a organização busca reduzir a probabilidade de ocorrência do risco ou minimizar seu impacto caso ele se materialize. O objetivo é tornar o risco menos provável ou, em alguns casos, removê-lo da lista de riscos críticos. Ex.: um risco referente a recebimento de brindes, presentes ou hospitalidades, onde podemos elaborar uma Política interna.

- **Evitar:** quando a organização altera processos ou atividades para impedir que o risco ocorra, ou para eliminá-lo completamente. Isso pode envolver interromper uma atividade ou suspender um processo que gera riscos significativos. Em alguns casos, quando a implementação de controles se torna financeiramente inviável, a única solução é evitar o risco, tornando a mitigação impossível.

Inicialmente, as medidas de resposta devem focar nas causas do evento de risco. Isso inclui ações preventivas para reduzir a probabilidade de ocorrência do evento e ações de contingência para minimizar o impacto caso um risco à integridade se materialize. Essas ações podem envolver a implementação de novos controles ou a otimização dos controles existentes, visando garantir a eficácia no tratamento dos riscos.

É importante ressaltar que as ações estabelecidas nas medidas de resposta aos riscos à integridade de uma Unidade podem envolver outras Unidades com as quais estejam relacionadas, desde que as partes envolvidas estejam em comum acordo.

As ações preventivas e de contingência devem ser aplicadas de forma diferenciada, conforme a estratégia escolhida como resposta para tratar os riscos à integridade, seja para mitigá-los, evitá-los ou transferi-los. A seguir, detalharemos como essas ações se aplicam em cada situação:

a) Riscos à integridade a serem mitigados:

- **Ações Preventivas:** São usadas para reduzir a probabilidade de ocorrência do risco ou para diminuir seu impacto, antes que ele aconteça. O objetivo é evitar que o risco se concretize ou minimize suas consequências, garantindo que a integridade da organização seja preservada. Exemplos: Implementação de treinamentos regulares sobre ética e

comportamento profissional para os agentes públicos, a fim de evitar práticas fraudulentas ou antiéticas; implementação de mecanismos de decisão colegiada na organização, compartilhando o poder de decisão; exigência de motivação detalhada nos casos em que houver discordância entre os posicionamentos de uma área técnica e da direção superior.

- **Ações de contingência:** Embora a mitigação busque reduzir o risco, ações de contingência podem ser necessárias caso o risco se concretize, mesmo após as ações preventivas. Essas ações visam minimizar os danos quando o risco ocorre, protegendo a integridade da organização. Exemplo: Se, após a implementação dos controles de integridade, ocorrer uma violação ética, as ações de contingência podem envolver a apuração do caso e a aplicação de medidas sancionatórias.

b) Riscos à integridade a serem evitados:

- **Ações preventivas:** Nesse caso, o objetivo é eliminar o risco completamente, ou seja, impedir sua ocorrência. As ações preventivas são adotadas para garantir que o risco nem mesmo surja. Isso pode envolver a modificação de processos, a interrupção de atividades ou a alteração de práticas que representem riscos à integridade. Exemplo: Se o risco envolver a possibilidade de um conflito de interesse, a ação preventiva seria a proibição de situações que possam gerar esse conflito, como garantir que agentes públicos não atuem em áreas onde possam ter interesses pessoais.

- **Ações de contingência:** Como o risco foi evitado, não são necessárias ações de contingência, já que não há possibilidade de o risco se concretizar. Nesse caso, não há necessidade de uma medida de resposta caso o risco aconteça.

c) Riscos a serem transferidos:

- **Ações preventivas:** Embora a transferência de risco movimente a responsabilidade para outra parte (como uma seguradora, no caso de riscos financeiros), ainda é necessário tomar ações preventivas para diminuir a probabilidade de o risco ocorrer ou minimizar seu impacto, especialmente se o risco não puder ser totalmente transferido. Exemplo: Se o risco de danos à imagem da organização por meio de vazamento de dados for transferido a uma empresa de segurança cibernética, as ações preventivas podem incluir a implementação de protocolos de segurança internos, como treinamento para agentes públicos sobre privacidade e proteção de dados.

- **Ações de contingência:** Para riscos transferidos, as ações de contingência podem ser necessárias, especialmente se a transferência não cobrir todos os aspectos do risco ou se o impacto for imediato. Por exemplo, em caso de um incidente de vazamento de dados, a organização pode ter que agir rapidamente, informar os stakeholders, e adotar medidas corretivas enquanto aguarda a compensação ou a ação da empresa responsável pela transferência do risco. Exemplo: Caso o seguro de responsabilidade civil não cubra totalmente os danos causados por um escândalo ético, a organização pode precisar de um plano de contingência para gerenciar a comunicação e lidar com a crise de imagem.

7.6 MONITORAMENTO, ANÁLISE CRÍTICA E MELHORIA CONTÍNUA

Esta etapa consiste no monitoramento e na análise crítica da eficiência e da efetividade da estrutura de gestão de riscos à integridade. O objetivo é promover a melhoria contínua, avaliando o desempenho das ações, corrigindo falhas de forma tempestiva e aprimorando os processos. Isso inclui a investigação e coleta de dados sobre a necessidade de aperfeiçoamento, treinamento de pessoas, redesenho de processos, atividades e rotinas, além da avaliação das ferramentas de trabalho, recursos e tecnologias utilizadas. O foco é garantir não apenas a eficácia no combate aos riscos à integridade, mas também promover ganhos contínuos no avanço da cultura e das ações de integridade.

A organização está sujeita a mudanças no cenário de riscos à integridade identificados. Por meio do monitoramento contínuo, é possível identificar novos riscos que possam surgir, além de avaliar os riscos existentes para verificar se houve alterações em sua probabilidade ou impacto. Esse processo também permite a redefinição da priorização dos riscos ou a eliminação de riscos previamente identificados. A análise da evolução dos riscos aceitos é igualmente fundamental, garantindo que esses permaneçam dentro de um nível aceitável ou que, se necessário, ajustes sejam realizados para mitigar possíveis impactos.

O monitoramento também envolve verificar se as ações previstas para o tratamento dos riscos à integridade estão sendo implementadas de forma adequada, considerando o tempo necessário para que as medidas atinjam seus objetivos e resultados esperados.

7.7 COMUNICAÇÃO E CONSULTA

A comunicação e consulta são componentes fundamentais no processo de gestão de riscos à integridade, e deve ser realizada de forma contínua ao longo de todo o processo. Trata-se de

manter um fluxo regular de informações entre as Unidades Funcionais do Coren-SC envolvidas, compartilhando dados relativos aos riscos à integridade identificados e às ações de tratamento adotadas.

Isso significa que todos precisam saber tudo sobre todos os riscos? Não necessariamente. A comunicação deve ser direcionada às partes interessadas. As pessoas ou áreas diretamente afetadas por um risco à integridade devem ser informadas, pois a materialização de um risco em uma Unidade Funcional pode impactar outras Unidades. Portanto, é essencial garantir que as informações pertinentes a cada risco à integridade sejam compartilhadas com as partes que possam ser afetadas.

As informações sobre os riscos devem ser acessíveis às partes interessadas, de forma clara, para que os envolvidos compreendam seus papéis e responsabilidades. Isso também cria uma base sólida para que todos possam atuar na gestão dos riscos à integridade de maneira eficiente e eficaz.

Esta etapa é crucial para garantir a transparência no processo, permitir a identificação adequada dos riscos à integridade, incorporar diferentes percepções e assegurar o apoio necessário para a implementação das ações de tratamento dos riscos.

7.7.1 Divulgação do Plano de Gestão de Riscos à Integridade

A implementação do Plano de Gestão de Riscos à Integridade requer ampla divulgação em todas as Unidades Funcionais do Coren-SC para que seja bem sucedida.

Após aprovação pelo Plenário do Coren-SC, o Plano de Gestão de Riscos à Integridade será disponibilizado na Plataforma Tecnológica de Compliance para conhecimento e assinatura de todos os agentes públicos do Conselho.

Uma reunião será agendada com os assessores das Unidades Funcionais, que serão responsáveis pela gestão dos riscos à integridade em suas respectivas Unidades, com o objetivo de apresentar o Plano e esclarecer eventuais dúvidas. A esses caberá repassar as informações pertinentes às suas equipes.

7.8 REGISTRO E RELATO

Os resultados do levantamento de riscos à integridade, incluindo todas as informações

coletadas nas etapas do processo de gestão de riscos durante as reuniões com as Unidades Funcionais do Coren-SC, serão devidamente registrados no módulo de Gestão de Riscos da Plataforma Tecnológica de Compliance.

A Encarregada da Gestão da Integridade do Coren-SC, na qualidade de Coordenadora do Processo de Gestão de Riscos à Integridade, encaminhará aos coordenadores das Unidades Funcionais um relatório detalhado contendo os riscos à integridade identificados em suas respectivas áreas, bem como o plano de ação proposto para o tratamento desses riscos.

Adicionalmente, será entregue à Alta Administração um relatório consolidado, abrangendo o levantamento dos riscos à integridade de todas as Unidades Funcionais do Coren-SC e os respectivos planos de alevalção para o tratamento dos riscos. O relatório será apresentado à Diretoria e ao Plenário para aprovação.

Caso a Alta Administração decida não adotar ações ou iniciativas para o tratamento de determinado(s) risco(s) à integridade identificados — seja por inviabilidade técnica ou financeira, relação custo-benefício da solução, entre outros — será necessário formalizar essa decisão por meio da assinatura de um Termo de Aceitação ao(s) Risco(s) (TAR). Esse termo deve identificar claramente o(s) risco(s) em questão, justificando a não adoção de medidas de tratamento.

8. REAVALIAÇÃO DOS RISCOS À INTEGRIDADE

Na Gestão de Riscos à Integridade, é essencial que os riscos sejam periodicamente reavaliados, pois as condições e os contextos podem mudar ao longo do tempo, seja devido a alterações internas no trabalho ou a fatores externos que impactem a organização.
A reavaliação dos riscos à integridade identificados nas Unidades Funcionais do Coren-SC será realizada por meio de novas reuniões com as respectivas Unidades Funcionais, com intervalos de um a dois anos, no máximo. O objetivo dessa reavaliação é:

- **Verificar a eficácia** das ações de tratamento adotadas para os riscos à integridade previamente identificados, avaliando se essas ações foram suficientes para reduzir o nível dos riscos;
- **Identificar a necessidade de novas ações de tratamento** para mitigar riscos à integridade que possam ter sido subestimados ou que tenham se intensificado com o tempo;
- **Detectar novos riscos à integridade** que possam ter surgido, e, caso necessário, iniciar o

ciclo completo das etapas do processo de gestão de riscos para tratá-los adequadamente.

Essa reavaliação garante que o processo de gestão de riscos à integridade permaneça dinâmico e atualizado, respondendo de forma eficaz a mudanças nas condições internas e externas que possam impactar a organização.

9. REFERÊNCIAS NORMATIVAS

- BRASIL. Tribunal de Contas da União. Manual de gestão de riscos do TCU/Tribunal de Contas da União. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2020. Disponível em https://portal.tcu.gov.br/data/files/46/B3/C6/F4/97D647109EB62737F18818A8/Manual_gestao_riscos_TCU_2_edicao.pdf

- BRASIL. Referencial básico de gestão de riscos/Tribunal de Contas da União. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018. Disponível em https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf

- BRASIL. Guia Prático de Gestão de Riscos para a Integridade. Orientações para a administração pública federal direta, autárquica e fundacional. Ministério da Transparência e Controladoria-Geral da União – Brasília, setembro/2018. Disponível em https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf

- BRASIL. Supremo Tribunal Federal. Guia de gestão de riscos/Supremo Tribunal Federal. Brasília: STF, Secretaria de Gestão Estratégica, Escritório de Gestão Aplicada, 2019. Disponível em https://www.stf.jus.br/arquivo/cms/centralDoCidadaoAcessoInformacaoGestaoEstrategica/anexo/GestaodeRiscos/GuiaGestaodeRiscos.pdf

- *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) – Gerenciamento de Riscos Corporativos – Estrutura Integrada. Disponível em https://auditoria.mpu.mp.br/pgmq/COSOIIERMExecutiveSummaryPortuguese.pdf

- BRASIL. Tribunal de Contas da União. Roteiro de Avaliação de Maturidade da Gestão de Riscos/Tribunal de Contas da União. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018. Disponível em https://portal.tcu.gov.br/data/files/0F/A3/1D/0E/64A1F6107AD96FE6F18818A8/Gestao_riscos_avaliacao_maturidade.pdf

- BRASIL. Portaria Controladoria Geral da União n.º 1.089/2018. Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências, disponível em https://www.gov.br/secretariageral/pt-br/estrutura/secretaria_de_controle_interno/arquivos/normativos/portaria-cgu-1089-2018.pdf/view e

posterior alteração por meio da Portaria Controladoria Geral da União n.º 57/2019, disponível em https://www.gov.br/prf/pt-br/canais-de-atendimento/ouvidoria/portaria-no-57-de-4-de-janeiro-de-2019.pdf

- BRASIL. Decreto n.º 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm

- Instrução Normativa Conjunta n. º 1, de 10 de maio de 2016 do Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Disponível em https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Normativos/instrucao-normativa-conjunta-no-1-de-10-de-maio-de-2016-imprensa-nacional.pdf/view

- Recomendações das melhores práticas internacionais que tratam da gestão de riscos corporativos, como o *Committee of Sponsoring Organizations of the Treadway Commission/ Enterprise Risk Management – Integrated Framework* (COSO/ERM) e as normas *The International Organization of Supreme Audit Institutions* (INTOSAI GOV9130/2007).

- ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. ENAP. Governança, gestão de riscos e integridade. James Batista Vieira, Rodrigo Tavares de Souza Barreto, Brasília: Enap, 2019.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000: Gestão de Riscos: Princípios e diretrizes, 1ª Edição, 2009.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31010: Gestão de Riscos: Técnicas para o processo de avaliação de riscos, 1ª Edição, 2012.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/GUIA 73: Gestão de Riscos: Vocabulário, 1ª Edição, 2012.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000: Gestão de Riscos: Diretrizes, 2ª Edição, 2018.

- Decisão Coren-SC n.º 030/2023, que dispõe sobre a Política de Gestão de Riscos do Conselho Regional de Enfermagem de Santa Catarina.

- Boletim do Tribunal de Contas da União Especial – v. 1, n. 1 (1982) – Análise SWOT e Diagrama de Verificação de Risco Aplicados em Auditoria – Brasília; TCU, 1982.

10. ANEXOS

ANEXO I - Plano de ação para execução do Processo de Gestão de Riscos à Integridade do Coren-SC;

ANEXO II - Modelo Termo de Aceitação ao(s) Risco(s) (TAR);

ANEXO III – Modelo planilha de levantamento dos processos de trabalho existentes.

ANEXO I - PLANO DE AÇÃO PARA EXECUÇÃO DO PROCESSO DE GESTÃO DE RISCOS À INTEGRIDADE DO COREN-SC

1. CRONOGRAMA

- Apresentação deste Plano à Diretoria - ROD (Reunião Ordinária de Diretoria) de setembro: 04/09/2025;
- Apresentação deste Plano para homolagação do Plenário – 654ª ROP (Reunião Ordinária de Plenário) de dezembro de 2025;
- Publicação do Plano na Plataforma de Compliance para ciência e assinatura de todos os agentes públicos do Coren-SC: assim que a Decisão aprovando o Plano for disponibilizada;
- Apresentação do Plano, após homologação em ROP, para Assessores: reunião de assessores de janeiro de 2026;
- Reunião com Diretoria para definição do apetite à riscos e posterior aprovação pelo Plenário: ROD e ROP de fevereiro de 2026;
- Envio do formulário às Unidades Funcionais para o levantamento dos processos de trabalho: 05/01/26, com prazo para resposta até 27/02/2026;
- Análise dos formulários, matrizes FOFA das Unidades e levantamento prévio dos riscos à integridade, a ser realizado pela coordenadora do processo de gestão de riscos à integridade: março a maio de 2026;
- Realização de reuniões com as Unidades Funcionais, entre junho e setembro de 2026, com o objetivo de identificar, analisar e avaliar os riscos à integridade de cada Unidade, bem como definir as medidas de tratamento mais adequadas. As datas serão agendadas em conjunto com a Coordenação das Unidades Funcionais, conforme disponibilidade;
- Entrega dos relatórios detalhados aos coordenadores das Unidades Funcionais, contendo os riscos à integridade mapeados relacionados à respectiva área, bem como o plano de ação para o tratamento dos riscos identificados: novembro/2026;
- Entrega e apresentação do relatório consolidado à Diretoria a ao Plenário do Coren-SC, abrangendo o mapeamento de riscos à integridade de todas as Unidades Funcionais do Coren-SC e os respectivos planos de ação para o tratamento dos riscos detectados: ROD e ROP dezembro/2026.

OBSERVAÇÃO: Este cronograma constitui uma previsão inicial e poderá ser ajustado, caso necessário.

2. ORDEM DAS REUNIÕES COM AS UNIDADES FUNCIONAIS

2.1 Divisão de Compras e Licitações (DCL);
2.2 Divisão Administrativa (DIAD);
2.3 Setor Financeiro;
2.4 Setor de Arrecadação;
2.5 Setor de Gestão de Pessoas;
2.6 Setor Contábil;
2.7 Departamento de Fiscalização do Exercício Profissional (DEFIS);
2.8 Cartório de Processos Éticos (CPROE);
2.9 Departamento de Registro, Inscrição e Cadastro (DRIC);
2.10 Departamento de Tecnologia da Informação e Comunicação (DTIC);
2.11 Gabinete e Presidente;
2.12 Plenário;
2.13 Superintendência;
2.14 Controladoria Geral (Conger);
2.15 Ouvidoria Geral;
2.16 Departamento Jurídico (DEJUR);
2.17 Assessoria de Comunicação (ASCOM);
2.18 Centro de Documentação e Memória (Cedoc);
2.19 Escritório de Gestão da Integridade (EGI).

OBSERVAÇÃO: A ordem das reuniões constitui uma previsão inicial e poderá ser alterada, caso necessário.

3. PASSO A PASSO DAS REUNIÕES COM AS UNIDADES FUNCIONAIS

3.1 Orientação à equipe da Unidade Funcional sobre a execução das etapas do processo de gestão de riscos à integridade, conforme estabelecido neste Plano, garantindo que todos os envolvidos compreendam suas responsabilidades e as ações a serem realizadas;

3.2 Apresentação dos riscos à integridade previamente identificados para a respectiva Unidade, com o objetivo de validar os riscos e, se necessário, adicionar outros que a equipe considere relevantes.

3.3 Para cada um dos **riscos à integridade identificados** serão realizados os seguintes **procedimentos**:

3.3.1 **Levantamento da(s) causa(s)** que pode(m) contribuir para a ocorrência do risco **e** da(s) possível (eis) **consequência(s)** sobre os objetivos, caso o risco se concretize;

3.3.2 **Cálculo do Nível de Risco Inerente (NRI) do risco,** por meio da mensuração da Probabilidade (P) e do Impacto (I), e do produto aritmético entre essas duas variáveis;

3.3.3 **Identificação do risco na matriz de riscos** para determinar sua classificação;

3.3.4 **Verificação da existência de controles internos** voltados para o enfrentamento do risco;

3.3.5 **Avaliação da eficácia dos controles internos,** com base na determinação do Fator de Avaliação dos Controles (FAC);

3.3.6 **Cálculo do Nível de Risco Residual (NRR),** por meio da multiplicação do NRI pelo FAC, seguido da definição da sua classificação;

3.3.7 Definição da **priorização do tratamento dos riscos,** com base no apetite ao risco definido pela Alta Administração;

3.3.8 Definição da(s) **medida(s) de resposta** ao risco;

3.3.9 Estabelecimento das **ações preventivas e de contingência** necessárias para tratamento do risco;

3.3.10 Designação dos **responsáveis por cada ação de tratamento** do risco;

3.3.11 Definição de **prazos** para a implementação das ações de tratamento.

ANEXO II – MODELO TERMO DE ACEITAÇÃO AO(S) RISCO(S) (TAR)

Identificação do(s) Risco(s) à Integridade e motivo(s) da aceitação

ID do Risco	Nome do Risco	Descrição do Risco	Unidade Funcional associada	Motivo(s) da aceitação
				( ) Inviabilidade técnica de mitigação;
				( ) Custo elevado em relação ao benefício esperado;
				( ) Risco considerado dentro dos limites aceitáveis pelo Coren-SC;
				( ) Ausência de alternativas viáveis de mitigação;
				( ) Outros: (Descrever).

Contexto

Este termo visa formalizar a decisão da Alta Administração do Coren-SC quanto à aceitação do(s) risco(s) à integridade acima identificado(s), conforme análise realizada pelo Escritório de Gestão da Integridade junto às Unidades Funcionais do Coren-SC.

Declaração de aceitação

A Alta Administração do Coren-SC, por meio deste instrumento, declara estar plenamente ciente da existência, natureza e possíveis impactos do(s) risco(s) à integridade acima identificado(s), e formaliza sua decisão consciente de aceitá-lo(s), assumindo a responsabilidade correspondente no âmbito de suas atribuições.

Determina-se, ainda, que o(s) risco(s) seja(m) monitorado(s) de forma contínua, com revisão obrigatória sempre que houver mudanças relevantes no cenário interno ou externo que possam alterar seu perfil ou gravidade.

Vigência e Acompanhamento

Este termo entra em vigor na data de sua assinatura e permanecerá válido até que haja alteração significativa do(s) risco(s) ou nova deliberação formal da Alta Administração. O acompanhamento e controle do(s) risco(s) será(ão) de responsabilidade dos gestores dos riscos juntamente com o Escritório de Gestão da Integridade.

(Local,data)

(Assinaturas)

ANEXO III – MODELO PLANILHA DE LEVANTAMENTO DOS PROCESSOS DE TRABALHO EXISTENTES

Ord.	Macroprocesso (é uma visão mais ampla e estratégica, que envolve vários processos menores e interligados)	Processo (é uma atividade ou tarefa específica, com um foco mais operacional e detalhado)	Meios/Recursos Utilizados (materiais, humanos, tecnológicos)	Pessoas envolvidas	Objetivos/ resultados a serem alcançados	Principais fatores internos que podem afetar o alcance dos objetivos/resultados	Principais fatores externos que podem afetar o alcance dos objetivos/resultados	Normativos (internos ou externos) aplicáveis aos processos de trabalho, caso existam	Periodicidade dos processos de trabalho (frequência com que são realizados e a média de duração, em termos de horas, dias, semanas, etc)
1									
2									
3									
4									
5									

Clique no link para acessar o formulário de levantamento dos processos de trabalho da Plataforma Tecnológica de Compliance:
https://beforms.becompliance.com/680f8b6f1ddfd000095d6ac4